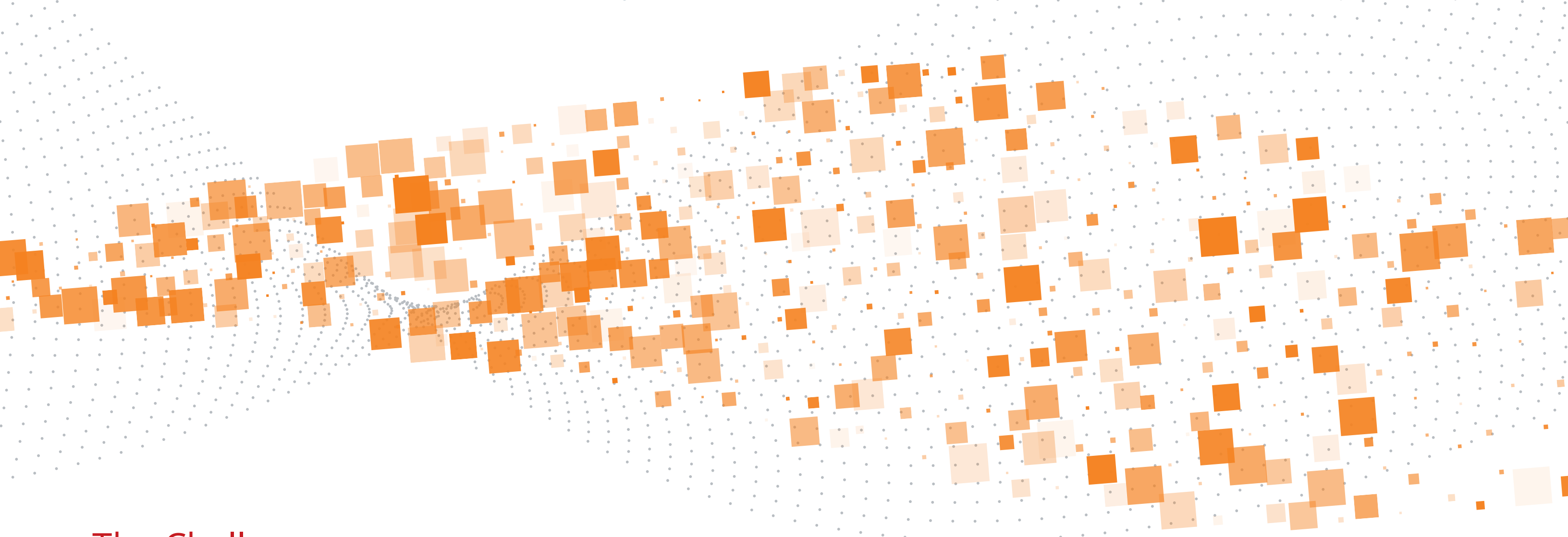
SOLUTION BRIEF

Cyber Threat Hunting Workshop

Learn from a real-world cyber threat scenario



The Challenge

Every year, governments and companies spend billions of dollars on cybersecurity and experienced teams work for countless hours, yet breaches are still depressingly routine. Why?

Preventing unauthorized access into, out of, or within a network requires understanding how that network is built– a difficult, tedious, and time consuming task.

Furthermore, trying to contain an incident without having full network context creates a high risk that an attacker will maintain a presence in your network. While your team focuses on analysis and containment, attackers can spread quickly and establish deep footholds across your network.

The Workshop

During the event, you will use the RedSeal platform and threat hunt within a pre-built virtual network model. You'll assess the network's overall cybersecurity posture while refining your skills in risk and vulnerability assessment, cyber hunting, and incident response.

At the completion of the session, you will have learned how to:
Identify potential attack vectors that bad actors could use to exploit existing vulnerabilities. Optimize resources by leveraging risk-based vulnerability prioritization.

> *"We are overwhelmed with data and underwhelmed by information. RedSeal allows us to prioritize with actionable intelligence and stop playing whack-a-mole."*
>
> **– DoD Customer**
>
> *"We have to be lean and agile as we execute our programs. We cannot keep the United States safe into the future, especially in the rapidly changing domain of cyber, using a firehose approach. We have to have the precision of a microsurgeon. We can't just be good; we have to be great. And, we can't be great without partnerships."*
>
> **– Adm. Michael S. Rogers**

Easily identify devices on the network that pose the most risk to your enterprise—those with network access and exploitable vulnerabilities.

Quickly visualize where bad actors can pivot following system compromise and traverse a network.

Coordinate with other teams to minimize the impact of an event while enhancing your organization's digital resilience. Use network context to develop mitigation strategies and implement your run-book plays.

RedSeal: The Must-Have Tool for Cyber Defenders

RedSeal understands and improves the resilience of every element, segment, and enclave of your network, enabling cyber defenders across government to carry out their missions. RedSeal works with your existing security stack and network infrastructure (including cloud and SDN) so you can automatically and continuously visualize a logical model of your "as-built" network.

RedSeal's cyber terrain analytics platform is designed to enable defenders to act with speed and efficiency. Forward cyber warriors defending the country have RedSeal in their toolkit; you can have it continuously on your network. With RedSeal, you can visualize end-to-end access, intended and unintended, between any two points of the network to speed incident investigation, auditing and compliance. You can visualize detailed access and attack paths for individual devices in the context of exploitable vulnerabilities to speed decision making, as cyber defenders do during a mission.

Who should attend

- Incident response and investigation teams
- Vulnerability managers and audit organizations
- Network and security operations teams
- Security engineers
- DOD cyber protection teams
- Current customers and partners

Battle Tested

RedSeal Department of Defense Clients

To register for a workshop, or for more information, go to https://www.redseal.net/cyber-threat-hunting-workshops/

ABOUT REDSEAL (redseal.net)

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.